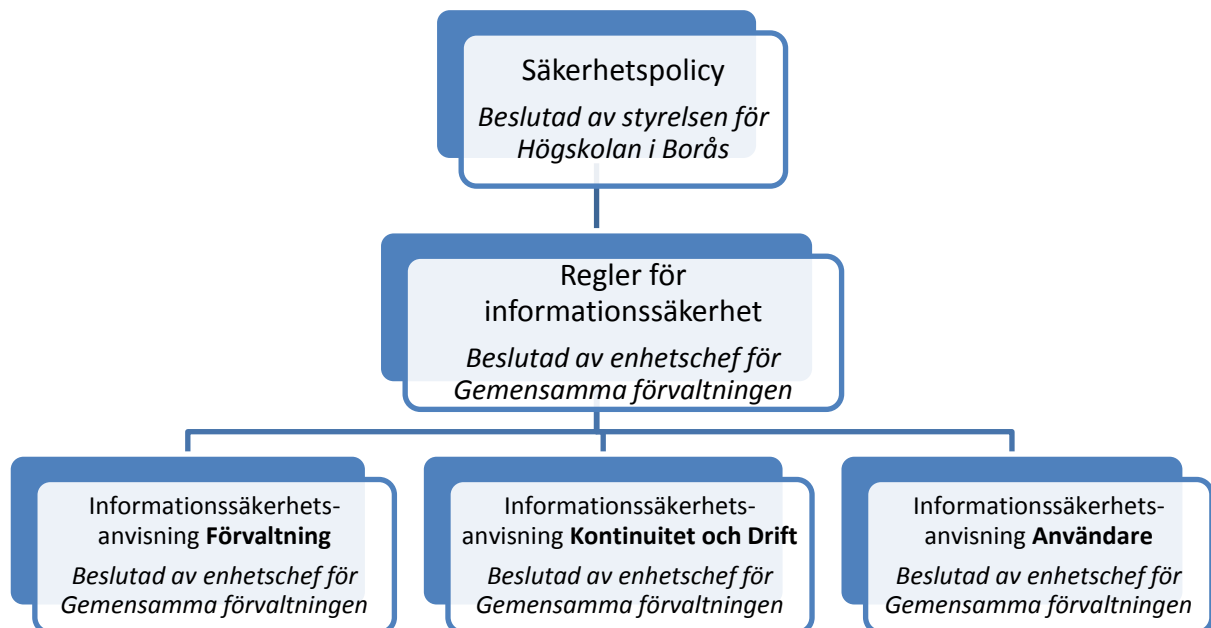


Regler för informationssäkerhet

Regler för informationssäkerhet är beslutade av enhetschefen för Gemensamma förvaltningen i enlighet med Högskolans säkerhetspolicy (dnr 288-11-101) samt rektors beslut från 16 februari 2010 (dnr 020-09-101). Gäller från och med 12 december 2012 och tillsvidare.

Ansvarig funktion för dokumentet: Höskolekansliet

Styrande dokument för informationssäkerhetsarbetet vid Högskolan i Borås:



Innehåll

1. Reglernas roll i informationssäkerhetsarbetet	3
2. Allmänt om informationssäkerhet.....	3
3. Roller och ansvar	4
4. Övergripande struktur för informationssäkerhet.....	4
4.1 Högskolans informationssystem	4
4.2 Informationsklassning	5
4.3 Kontinuitetsplanering	5

1. Reglernas roll i informationssäkerhetsarbetet

Säkerhetspolicyn redovisar Högskolans viljeinriktning och mål för det övergripande säkerhetsarbetet, vari informationssäkerheten är en del.

Regler för informationssäkerhet redovisar roller och övergripande struktur för informationssäkerheten.

Informationssäkerhetsanvisning **Användare** redovisar hur varje enskild användare ska verka för att upprätthålla en god informationssäkerhet.

Informationssäkerhetsanvisning **Förvaltning** redovisar:

- Det ansvar som ingår i de olika rollerna
- De regler som gäller för områden av särskild betydelse
- Regler för nyanskaffning, underhåll, förändrings- och incidenthantering

Informationssäkerhetsanvisning **Kontinuitet och Drift** redovisar:

- Organisation och ansvar för informationssystem
- Regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

2. Allmänt om informationssäkerhet

Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Säkerhetspolicyn med tillhörande regler för informationssäkerhet styr högskolans informationssäkerhetsarbete. I säkerhetspolicyn anges att målet med informationssäkerhet är att säkerställa sekretess, riktighet, tillgänglighet och spårbarhet för verksamhetens informationstillgångar.

Information är en viktig tillgång för högskolan och hanteringen av den är en viktig del i arbetet med högskolans risk- och sårbarhetsanalys.

Utgångspunkter i högskolans arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Högskolans egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar högskolans informationstillgångar utan undantag. Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt,
- att informationen är och förblir riktig.

Informationssäkerheten är en integrerad del av högskolans verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för högskolans informationstillgångar.

Alla delar inom högskolan är bundna av dessa regler för informationssäkerhet vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från dessa eller de säkerhetsinstruktioner som beslutats av behörig beslutsfattare.

Den som använder högskolans informationstillgångar på ett sätt som strider mot dessa regler kan bli föremål för disciplinära åtgärder.

3. Roller och ansvar

Rektorn eller den denne utser har det övergripande ansvaret för informationssäkerheten.

Informationssäkerhetssamordnaren har det operativa ansvaret för samordning av informationssäkerhetsarbetet samt ansvar för att dessa regler revideras vid behov.

Prefekt eller enhetschef ansvarar – enligt beslut fattat den 16 februari 2010 (dnr 020-09-101) – för att klassning och riskanalyser genomförs i enlighet med av Informationssäkerhetssamordnarens beslutade instruktioner.

Systemägaren är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer.

Systemförvaltarna ansvarar för den dagliga användningen av informationssystemen.

IT-chefen ansvarar för att uppfylla högskolans kontinuitetsplan för IT-stödet.

Användare ansvarar för att följa gällande regler.

4. Övergripande struktur för informationssäkerhet

4.1 Högskolans informationssystem

Högskolans informationssystem ska vara identifierade, förtecknade och informationsklassade. Av förteckningen ska framgå vem som är systemägare.

4.2 Informationsklassning

Högskolans informationssystem ska vara klassificerade utifrån aspekterna sekretess, riktighet och tillgänglighet. Klassificeringen ska utgå från den information som hanteras i systemet.

Högskolans klassningsmodell framgår av bilaga *Informationssäkerhetsanvisningar – Användare*.

För de system som klassificeras lägst Klass 2 vad gäller sekretess eller riktighet ska en riskanalys genomföras i enlighet med gällande instruktioner. Till riskanalysen ska en handlingsplan fogas visande hur identifierade risker ska beaktas och hanteras. Riskanalysen ska kontinuerligt uppdateras och rapporteras till Informationssäkerhetssamordnaren i enlighet med gällande instruktioner.

4.3 Kontinuitetsplanering

Kontinuitetsplaneringen är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska finnas för driften av IT-stöd baserad på de olika informationssystemens samlade krav utifrån gjord informationsklassning.